PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-318036
(43)Date of publication of application : 15.11.1994

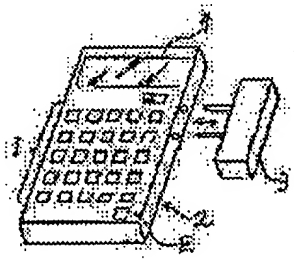
(51)Int.Cl. G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-098232
(22)Date of filing : 11.04.1994
(Divisional filing date)

(71)Applicant : TSUKAMOTO YUTAKA
(72)Inventor : TSUKAMOTO YUTAKA

(54) DIGITAL SIGNATURE SYSTEM

(57)Abstract:
PURPOSE: To prevent the trouble that a secret rule leaks to the outside by converting sent data by a personal terminal device according to algorithm based upon the secret rule.
CONSTITUTION: Plural mutually different kinds of secret rule are stored in the personal terminal device 3 and then when respective signers who are going to sign. personal terminal device 3, have these respective signers have own inherent secret rule. For digital signing, the sent data of characters, etc., of a contract to be an object of signature are inputted from a keyboard 1 in the form of HIRAGANA (cursive form of Japanese syllabary) while the personal terminal device 3 is mounted on the input device 2. Converted data as an answer consisting of ciphered codes are displayed as signature data on a display part 4 and the signature data are sent along with the sent data on the contract, etc., to be an object of recognition. Then the converted data are so transmitted that a receiver side can be discriminated from the sent data.



LEGAL STATUS

[Date of request for examination]	11.05.1994
[Date of sending the examiner's decision of rejection]	30.09.1997
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2967456
[Date of registration]	20.08.1999
[Number of appeal against examiner's decision of rejection]	09-18535

[Date of requesting appeal against examiner's decision of rejection] 30.10.1997

[Date of extinction of right] 16.02.2001

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平6－318036
(43)公開日　平成６年(1994)11月15日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ	1/00		8837－5L		
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
			8949－5K	Ｈ０４Ｌ　9/00	Ｚ

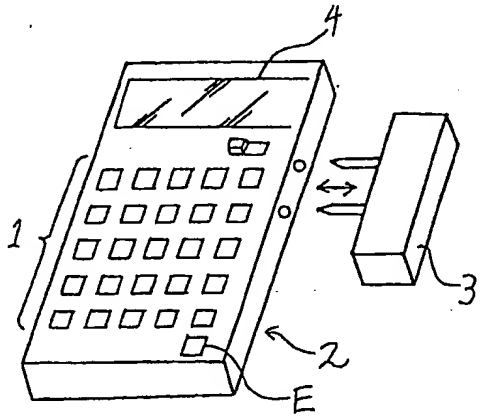
審査請求　有　発明の数１　ＦＤ（全 11 頁）

(21)出願番号　特願平6－98232
(62)分割の表示　特願昭59－213688の分割
(22)出願日　昭和59年(1984)10月11日

(71)出願人　593187342
塚本　豊
岡山県玉野市玉４丁目８番20
(72)発明者　塚本　豊
岡山県玉野市玉４丁目８番20号

(54)【発明の名称】　ディジタル署名システム

(57)【要約】
【目的】　ディジタル署名システムにおける秘密鍵等の秘密ルールの漏洩を防止する。
【構成】　物理的に安全な装置であるパーソナル端末装置３に秘密ルールを記憶させ、パーソナル端末装置３内部で秘密ルールを用いた暗号化等の変換動作を行なわせる。



1

【特許請求の範囲】

【請求項1】　署名を行なう対象である所定の送信データを通信によりやり取りして署名を行なうディジタル署名システムであって、

前記送信データに対し署名を行なわんとする署名者が所有する署名者固有の秘密のルールを記憶し、該秘密ルールに従ったアルゴリズムにより前記送信データを変換する変換機能を有し、前記署名者所有のパーソナル端末装置と、

該パーソナル端末装置に前記送信データを入力するデータ入力手段とを含み、

前記データ入力手段により入力されて前記パーソナル端末装置により変換された変換データを、受信者側が前記送信データと区別できるように前記受信者側に送信することによりディジタル署名を行なうことを特徴とする、ディジタル署名システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、主として、異なった企業間同士で、テレテックス等の送信装置を使用して、取引に伴う注文書や契約書の内容等の送信データを当事者のコンピュータ間でやり取りしてペーパレスの取引を行なう場合に、その取引契約内容である送信データの認証のための署名を行なう場合に使用するディジタル署名システムに関する。

【0002】

【従来の技術】従来の紙に記載された契約書を取り交わして署名を行なう場合には、印鑑やサイン等によりその契約交渉の正当性を認証していた。ところが、特に利害関係のある契約内容等のデータがペーパレスによる電子化取引のように通信でやり取りされる場合には、サインや印鑑の印章をそのままディジタル信号に変換して送信しても、そのディジタルからなる署名データが相手側の電子ファイル等に記憶されることとなり、その記憶された署名データが他のペーパレス契約書類に多数コピー使用されるおそれが生ずる。すなわち、相手側によって記憶された署名データが他の契約書に悪用されて被害を被るおそれが発生するのであり、印鑑等が盗まれたのと同様の不都合な事態が発生することになる。

【0003】さらに、このようなペーパレス取引においては、契約締結後における契約内容の改ざんがコンピュータ端末上の操作で容易にでき、しかも、何ら改ざんの痕跡が残らないために、改ざんが多発するおそれがあるとともに、その改ざんを発見して取り締まることが非常に困難となる欠点が生ずる。

【0004】

【発明が解決しようとする課題】そこで、上述した欠点を解消するべく、次のようなディジタル署名システムを採用することが考えられる。

【0005】図11に示すものは、本発明の背景となる

2

技術の一例であり、公開鍵暗号方式を利用したディジタル署名の一例である。受信者Aが署名せんとする送信データの一例のメッセージMを自己が所有する秘密の復号鍵D_Aにより復号化してD_A（M）を得、さらにその復号化されたデータD_A（M）を、相手方すなわち受信者Bの公開鍵E_Bで暗号化し、暗号文C＝E_B（D_A（M））を得る。そしてこの暗号文Cを受信者Bに送信する。受信者Bでは、受信データCを自己が所有する秘密鍵D_Bで復号化してD_A（M）を得る。このD_A（M）が署名データとなる。そして、D_A（M）を公開鍵E_Aで暗号化することにより元のメッセージMを得ることができる。受信者Bでは、このメッセージMとともに前記D_A（M）を署名データとして電子ファイル等に記憶して保存しておく。

【0006】このように、メッセージ等の送信データを署名せんとする署名者が所有する対外的に秘密な秘密鍵D_A等からなる秘密ルールに従って、前記送信データを変換し、その変換データD_A（M）を受信者側が前記送信データMと区別できるように受信者側に送信することにより、ディジタル署名を行なうことが可能となる。その結果、受信者Bにおいて、受信したデータMを改ざんした場合には、データMと署名データであるD_A（M）との整合性がなくなり、両者がちぐはぐなものとなってしまう。すなわち、署名データであるD_A（M）とは、データMを送信者Aの秘密鍵D_Aで復号化したものであり、このデータMが改ざんされた後のデータをM′とした場合には、このM′を前記秘密鍵D_Aで復号化したとしてもD_A（M′）となり、前記D_A（M）と一致しない状態となり、改ざんされたことが容易に判明されるのである。そこで、受信者Bにおいては、データMを改ざんするとともに、その署名データD_A（M）の方も、改ざんしたデータであるM′に対し整合性のとれたD_A（M′）に改ざんして、両者の間の整合性が保たれるように偽造を試みるが、しかし、受信者B側が前記D_A（M′）を得るためには、送信者Aの秘密ルールの一例の秘密鍵D_Aがわからない限り不可能なのである。ところが、この秘密鍵D_Aは対外的に秘密であるとともに送信者A固有の鍵であるために、受信者Bが秘密鍵D_Aを得ることは一般的に不可能なのである。また、この受信者Bが受信した署名データであるD_A（M）を他のペーパレス契約に転送せんとしても、他のペーパレス契約内容は一般的に前記データMとは異なっているために、その異なった内容であるデータNに対し署名データであるD_A（M）をコピー使用せんとしても、データNと署名データD_A（M）との間で整合性がとれないために、署名データの他の契約への転用が容易に判明できるのである。

【0007】以上説明したように、図11に示したディジタル署名システムは、送信データMに対し署名を行なわんとする署名者Aが所有する秘密鍵D_A等の対外的に

秘密の秘密ルールに従ったアルゴリズムにより前記送信データMを暗号化等の所定の変換を行ない、その変換データD_A（M）を受信者Bが前記送信データMと区別できるように受信者側Bに送信することによりディジタル署名を行なうものであり、前記署名データD_A（M）と送信データMとの間で受信者側Bが見破ることのできない一定の相関関係を持たせることにより、ペーパレス取引等における署名機能を発揮できるのである。

【0008】しかし、このようなディジタル署名システムにおいては、前記秘密鍵D_A等の秘密ルールの秘密性を守ることが重要であり、この秘密ルールが漏れて受信者側Bに知れてしまった場合には、受信者側Bにおいては、データMを改ざんするとともに、署名データの方もその改ざんされたデータに対し前記一定の相関関係を有するものに改ざんすることが可能となり、ディジタル署名としての機能を全く有しなくなるのである。

【0009】本発明は、係る実情に鑑み考え出されたものであり、その目的は、ディジタル署名システムを利用してディジタル署名を行なうにおいて、前記秘密ルールの秘密性を守りその秘密ルールが対外的に漏れてしまう不都合を極力防止できるディジタル署名システムを提供することである。

【0010】

【課題を解決するための手段】本発明は、署名を行なう対象である所定の送信データを通信によりやり取りして署名を行なうディジタル署名システムであって、前記送信データに対し署名を行なわんとする署名者が所有する署名者固有の秘密のルールを記憶し、該秘密ルールに従ったアルゴリズムにより前記送信データを変換する変換機能を有し、前記署名者所有のパーソナル端末装置と、該パーソナル端末装置に前記送信データを入力するデータ入力手段とを含み、前記データ入力手段により入力されて前記パーソナル端末装置により変換された変換データを、受信者側が前記送信データと区別できるように前記受信者側に送信することによりディジタル署名を行なうことを特徴とする。

【0011】

【作用】本発明によれば、送信データに対し署名を行なわんとする署名者が所有するパーソナル端末装置に対し、データ入力手段により前記送信データが入力される。そして、パーソナル端末装置においては、署名者が所有する署名者固有の秘密ルールが記憶されており、その秘密ルールに従ったアルゴリズムにより前記入力された送信データが変換される。そして、その変換データが、受信者側が前記送信データと区別できるように受信者側に送信されてディジタル署名が行なわれる。

【0012】

【発明の実施例】図１に示すように、文字用キーと数字用キーにより平仮名と数字をインプットできるキーボード１を有するデータ入力手段の一例のデータ入力装置２に対し、ＲＡＭやＣＰＵ内蔵のパーソナル端末装置３を着脱自在に構成している。このパーソナル端末装置はディジタル署名をせんとするデータの送信者が個人的に所有する装置であればどのようなものであってもよく、従来から一般的に周知なものとしては、たとえばＩＣカード等が考えられる。

【0013】この個人所有のパーソナル端末装置３の回路構成を図１０に示す。パーソナル端末装置３内には、ＣＰＵ５０と、ＲＯＭ５１と、ＲＡＭ５２と、Ｉ／Ｏポート５３とが設けられている。ＲＯＭ５１は、ＣＰＵ５０の動作プログラムすなわち後述する図２に示すフローチャートのプログラム等が記憶されている。ＣＰＵ５０は、そのＲＯＭ５１に記憶されているプログラムに従って動作し、後述する秘密ルールの一例の文字数字変換ルールやシークレット関数を呼出してＲＡＭ５２に記憶させる。そして、後述するように、キーボード１から入力されてＩ／Ｏポート５３から入力された送信データを、ＲＡＭ５２に記憶されている秘密ルールに従ったアルゴリズムにより、図２に示すように変換し、その変換データをＩ／Ｏポート５３から出力する。

【0014】このパーソナル端末装置３に記憶されている秘密ルールは、平仮名文字を一定のルールに従って数字に変換するための文字数字変換ルールと、三角関数，指数関数等の組合せからなるシークレット関数ｆ（ｘ）等から構成されている。この秘密ルールはパーソナル端末装置３においてそれぞれ相違した種類のものが記憶され、そのため、署名せんとする各署名者がそれぞれこのパーソナル端末装置３を所有することによって、各署名者はそれぞれ自己固有の秘密ルールを保有することになる。また、この秘密ルールは対外的に秘密なものである。

【0015】そして、前記パーソナル端末装置３には、図２に示すフローチャートのプログラムが組込まれており、ディジタル署名を行なう場合には、前記パーソナル端末装置３を入力装置２に装着した状態で署名対象である契約書の文字等の送信データを平仮名の形でキーボード１から入力する。また、日付等の数字はそのまま入力する。そして、入力されたものが文字である場合には、前記文字数字変換ルールに従って入力毎に逐一文字を数字に変換して足し合わせ、さらに、入力されたものが数字である場合には、その数字をそのままの形で足し合わせ、次にＥＮＤ用キーＥのＯＮ操作があれば、すべての文字，数字の和Ｐ（ｎ）を前記シークレット関数ｆ（ｘ）に代入して答を算出し、その暗号化された符号からなる答である変換データ（この場合は数字となる）を署名データとしてＩ／Ｏポート５３から出力して表示部４に表示させる。そして、その表示部４に示された署名データを認証対象となる契約書等の送信データとともに送信する。

【0016】前記入力装置２は、テレテックス端末機で

5

あってもよく、その場合には、署名対象物である送信データをテレテックス端末機のキーボードからパーソナル端末装置３に入力する。また、パーソナル端末装置３から出力された変換データである認証データを契約相手にテレテックス端末機から伝送するよう構成する。

【００１７】さらに、前記文字数字変換ルールとシークレット関数とからなる秘密ルールは、秘守義務のある官公庁等の公共機関やサービス機関等に登録しておく。

【００１８】書類受付印，受理印，金銭領収印のように、チェックのための認証を行なうディジタル署名の場合には、書類受付行為等の認証対象行為自体を平仮名文字でキーボード１から入力し、さらに、認証対象行為を行なった日付を入力して変換データすなわち署名データを算出する。たとえば、認証対象行為が書類受付であり、認証日付が１９８４年１０月９日１１時３５分であれば、キーボード１に、「しょるいうけつけ１９８４ねん１０がつ９ひ１１じ３５ふん」と入力する。

【００１９】また、書類受付行為，受理行為等の種々の代表的チェック行為をキーボード１における１つの操作ボタンに割り付けることによってワンタッチで入力できるように構成してもよい。

【００２０】さらに、本発明でいう認証対象行為として挙げた書類受付行為，受理行為等は単なる例示であり、その他、注文書，納品書，領収書等への認証における注文行為，品物納入行為，金銭領収行為等、種々のチェック行為が含まれることは言うまでもない。

【００２１】次に、本発明の別実施例を説明する。

② シークレット関数によって算出された数字をそのまま署名データとする代わりに、その算出された数字の一部または全部を、一定のシークレットなルールに基づいて、平仮名，片仮名，漢字アルファベット等の文字や、図形，記号またはそれらの組合せまたはそれらと色彩との組合せに変換して署名データとして用いる。

【００２２】③ 前記秘密ルールをパーソナル端末装置３に記憶させる代わりに、図３に示すように、企業等のファイル装置５に記憶させておく。その場合には、テレテックス端末機６と前記ファイル装置５とをコンピュータ７を介してＬＡＮ８等で接続し、公衆回線等を利用して他の企業との間で行なわれるペーパレス取引の署名者が、自己の秘密ルールを前記テレテックス端末機６からの操作で呼出し、前記コンピュータ７によって暗号化等の変換作業を行なう。前記秘密ルール呼出しの際には、後述する個体識別システムを利用して、署名者が呼出指定している秘密ルールが本当にその署名者のものであるか否かをコンピュータ７によりチェックし、署名者のものであることが確認できた段階で初めて呼出指定された秘密ルールへのアクセスを可能にする。

【００２３】なお、図中９はノードである。

④ 秘密ルールを企業内のファイル装置５から呼出す代わりに、秘密ルールが登録されている公共機関やサービス機関等のファイル装置、または、自宅のファイル装置からデータ通信により自己の秘密ルールを呼出し、その呼出したファイル装置に接続されているコンピュータで暗号化等の変換作業を行なう。

【００２４】⑤ 前記パーソナル端末装置３を、その装置所有者が所有する発信機（たとえば指輪型のもの）からの所定の信号（発信機それぞれによって相違する）を受信できなくなれば、暗号化等の変換機能が停止するように構成し、パーソナル端末装置３の紛失時における他人の悪用を防止できるようにする。

【００２５】⑥ 暗号化等の変換方法として、図２に示したＰ（Ｎ）＝Ｐ（Ｎ－１）＋Ｄ（Ｎ）の代わりに、Ｐ（Ｎ）＝Ｐ（Ｎ－１）＋Ｎ・Ｄ（Ｎ）、Ｐ（Ｎ）＝Ｐ（Ｎ－１）＋Ｄ（Ｎ）／Ｎ、Ｐ（Ｎ）＝Ｐ（Ｎ－１）／Ｎ＋Ｄ（Ｎ）、あるいは、Ｐ（Ｎ）＝Ｐ（Ｎ－１）／Ｎ＋Ｎ・Ｄ（Ｎ）等を用いる。

【００２６】次に、本発明とは直接関係はないが、たとえば、前述したように、秘密ルール呼出しの際に呼出指定された秘密ルールが本当に本人のものであるか否かを判別する個体識別システムの発明について説明する。

【００２７】この発明は、主として、或る設備へのアクセスを限られた者にのみ限定するべく、整備へのアクセスが許されるべき者か否かを判別するものであり、詳しくは、或る一定の入力信号をインプットされた場合に、一定のシークレットなルールに基づいて答えを算出し、それを識別信号としてアウトプットする設備利用者所有の装置３３と、或る一定のシークレットルールが登録され、そのシークレットルール（秘密ルール）と前記入力信号とから前記アウトプットされた識別信号が正しいものであるか否かを判断する判断手段とを有する個体識別システムに関する。

【００２８】この種の個体識別システムにおいて、従来、一般的に使用されているものに、たとえば、特開昭５９－１０６８０号公報に記載の技術があり、利用対象設備に一定のシークレットルールを前もって登録しておき、或る一定の入力信号に基づき、設備利用者所有の装置によって算出された識別信号と、前記利用対象設備で算出された識別信号とが一致する場合にのみ、前記装置所有者を設備へのアクセスが許容できるものと判断するのである。

【００２９】ところが、高度情報化社会となり、この種の個体識別システムが普及した場合には、たとえば、コインロッカのドアの解錠、自己の銀行口座の呼出し、使用者が限定されているシークレットな技術情報のファイル装置等からの呼出し等、本システムの使用頻度が増大し、多くの利用設備へのアクセスに使用されることになるのであり、そのために、自分が利用する多くの利用設備すべてに逐一シークレットルールを登録しなければならず、それだけ登録されたシークレットルールの他人による盗用の機会が増大し、悪用による多大な損害が発生

するという欠点が生ずる。特に高度情報化社会においては、個人のプライバシーや企業秘密の漏洩は万が一にもあってはならないのであり、シークレットルールの盗用は厳に防止しなければならないのである。

【００３０】そこで、利用設備毎に異なったシークレットルールを登録し、たとえばそのうちの１つのシークレットルールが盗まれたとしても、他の利用設備へのアクセスに悪用されないようにする方法も考えられるが、設備毎に使用対象とするシークレットルールを設備利用者が記憶しておかなければならず、煩雑であり、特に、利用対象設備が多くなれば忘れる可能性もあり、不都合である。

【００３１】この個体識別システムの発明の目的は、上記実情に鑑み、利用設備が多くなったとしても、多くのシークレットルールの登録を行なうことなく、登録したシークレットルールの盗用による損害の発生の増大を防止し得る個体識別システムを提供する点にある。

【００３２】上記目的を達成するべくなされた個体識別システムの構成は、システム使用時に前記シークレットルール登録場所と利用設備等をデータ通信可能な状態になるように前もって設定する設定手段を設け、利用設備から伝送されてきた識別信号が正しいものであるか否かの判断を前記シークレットルール登録場所で行なう点である。

【００３３】このような構成を有する個体識別システムの発明の作用効果は、以下のものである。

【００３４】つまり、本システム使用時においては、設備利用者所有の装置からアウトプットされた識別信号が利用設備を通じてデータ通信によりシークレットルール登録場所まで伝送されてくるのであり、そのシークレットルール登録場所でその送られてきた識別信号が正しいものか否かを判断でき、そのために、個体識別をしなければならない利用設備が多数存在したとしても１箇所にのみ登録された１つのシークレットルールに基づいての個体識別が可能であり、利用設備の増大に伴うシークレットルールの盗用の増大化を防止し得るのであり、盗用に伴う損害の発生の増加を防止し得るに至った。

【００３５】なお、前記データ通信は、有線系メディア，無線系メディアの両方を含む。次に、同じ個体識別システムの発明であるが、前述のものとは相違する発明を以下に述べる。

【００３６】この発明も、前述の発明と同様の利用分野をもち、目的もシークレットルールの盗用防止という点で前述の発明と共通するのであるが、前発明がシークレットルールの登録場所の増加に伴う盗用の増加に対処したものであるのに対し、この発明は、シークレットルールの使用頻度の増加に伴うシークレットルール盗用の増加に対処せんとするものである点が相違する。

【００３７】つまり、利用設備が増加し、シークレットルールの使用頻度が増加した場合には、シークレットルール自体が盗用不可能だとしても、本システムを悪用せんとする者によって、入力信号とそれに対応する識別信号を本システム使用毎に逐一シラミ潰し的に記録され、その記録量が膨大なものとなれば、悪用者が本システムを使用するに際して、任意に選出された入力信号が偶然に悪用者によって過去に記録されたものの中に存在し、設備へのアクセスが悪用者に許容されてしまうという可能性も生じてくるのであり、本システムの使用頻度が高まれば、いくらシークレットルールの盗用を厳重に防止したとしても悪用者による損害が発生する危険性が生ずる欠点がある。

【００３８】この発明の目的は、上記実情に鑑み、システムの使用頻度が増大し、悪用者による入力信号とそれに対応する識別信号のシラミ潰し的な記録にもかかわらず、悪用者の利用設備へのアクセスを有効に防止し得る個体識別システムを提供する点にある。

【００３９】このような目的を達成するべくなされた個体識別システムの発明の構成は、或る一定の入力信号をインプットされた場合に、一定のシークレットなルールに基づいて答えを算出し、それを識別信号としてアウトプットする設備利用者所有の装置３３と、或る一定のシークレットルールが登録され、そのシークレットルールと前記入力信号とから前記アウトプットされた識別信号が正しいものであるか否かを判別する判別手段とを有する個体識別システムにおいて、入力信号として、未だに使用されたことのないものを使用する選択使用手段を有する点にある。

【００４０】上記構成を有する個体識別システムの発明の作用効果は、以下のものである。つまり、悪用者によって入力信号と識別信号とを逐一シラミ潰し的に記録されたとしても、過去において一旦使用された入力信号は二度と使用されないために、前述した記録を利用した悪用は不可能となり、本システムの使用頻度が増大した場合にも、システムの悪用を確実に防止でき、プライバシーや企業秘密の漏洩防止という高度情報化社会における宿命的課題に十分応えることのできる個体識別システムを提供し得るに至ったのである。

【００４１】次に、この個体識別システムの発明の実施態様を以下に列記する。

② 前記選択使用手段として、過去において使用されたことのある入力信号を拒絶する機能を前記判断手段側に持たせた個体識別システム。

【００４２】③ 前記選択使用手段として、全国共通でしかも選択使用毎にまたは経時的に増加または減少する数字を前記入力信号として用いた個体識別システム。

【００４３】④ 前記数字が、コード／データ放送によって伝送されてきた信号に基づいて定められたものである、前記第③項記載の個体識別システム。

【００４４】⑤ 前記数字が、現在の年月日時刻を表わすものである前記第③項または第④項記載の個体識別シ

ステム。

【００４５】⑥　前記設備利用者の装置が腕時計で構成され、その腕時計が表示されている時刻を入力信号として使用する前記第③項記載の個体識別システム。

【００４６】⑦　前記腕時計が、コード／データ放送によって伝送されてきた信号に基づいて時刻表示可能なものである前記第⑥項記載の個体識別システム。

【００４７】⑧　前記コード／データ放送が、利用対象となる各々の設備から発信されているものである前記第④項または第⑦項記載の個体識別システム。

【００４８】⑨　前記腕時計が、アウトプットされた識別信号を人間の手を媒体として利用対象設備側に伝送するべく、人間の手への信号送出し部を有する前記第⑥項または第⑦項記載の個体識別システム。

【００４９】⑩　前記設備利用者所有の装置が、その装置所有者が所有する発信機からの所定の信号を受信できなくなれば、個体識別のための機能が停止するもので構成されている個体識別システム。

【００５０】次に、前述した個体識別システムの発明も含め、個体識別システムの発明の実施例を図面に基づいて説明する。

【００５１】図４に示すように、銀行１０内の自己の口座の呼出し、データバンク１１内のシークレットな技術情報の検索、コインロッカ１２の解錠等、一定の限られたものにのみアクセスを許容するべき設備と、設備利用者にアクセスを許容してもよいか否かの個体識別を判断する自宅または所定の機関のコンピュータ１３または１４とを公衆回線１５で接続し、それら設備１０，１１，１２と個体識別を行なうコンピュータ１３，１４との間でデータ通信が可能になるように構成している。また図中１６は網制御装置（ＮＣＵ）、１７は交換機である。

【００５２】そして、たとえば、データバンク１１内の技術情報を利用したい場合には、まず、キャプテン用端末機１８により、データバンク１１を呼出して所望の技術情報を検索してもらい、その技術情報が或る一定のものにしか使用許可されないシークレットな技術情報である場合には、以下の手順で個体識別を行なう。

【００５３】②　技術情報を使用せんとする設備利用者が個体識別を行なう自宅または所定機関のコンピュータ１３または１４の呼出番号をデータバンク１１に知らせる。

【００５４】③　データバンク１１側は、その番号が前もって登録されている使用許可できるものの番号であるか否かを確認し、使用許可者の番号であれば識別信号の送信を要求し、使用許可者の番号でなければ使用を許可しない。

【００５５】④　前記識別信号の送信要求がでれば設備利用者は自己所有の装置３３からアウトプットされた識別信号をキャプテン用端末機１８によりデータバンク１１側に送信する。

【００５６】⑤　データバンク１１側は送信されてきた識別信号を前記呼出番号のコンピュータ１３または１４に送信し、そのコンピュータ１３または１４で送信されてきた識別信号が正しいものか否かの個体識別判断（後述する）を行ない、その結果をデータバンク１１側に送信する。

【００５７】⑥　データバンク１１側では、正しいという判断結果が送信されてきた場合にのみ呼出指定されているシークレット技術情報へのアクセスを許可する。

【００５８】次に、コインロッカ１２を解錠する場合の手順は、まず、解錠状態にあるコインロッカのドア内面側にあるキーボードの操作によって個体識別を行なう自宅または所定機関のコンピュータ１３または１４の呼出番号をインプットし、予め前記コンピュータ１３または１４を登録し解錠操作時に自動的にそのコンピュータ１３または１４が呼出されるように設定した状態でドアを閉じて錠をかけ、解錠時には、そのコインロッカのドア外面から識別信号をインプットし、前述した⑤，⑥と同様の方法により解錠制御を行なう。

【００５９】次に、たとえば、金銭の支払いに際して、自己の銀行口座の預金を金銭受取人の銀行口座内に移動させるという数字の移動のみで現金の移動を伴わないキャッシャレス支払システム（銀行ＰＯＳシステム）等において、自己の銀行口座を呼出す手順は、まず、銀行に前もって自宅または所定機関のコンピュータ１３または１４の呼出番号を登録しておき、自己の銀行口座の呼出指定があった場合には、自動的に前記コンピュータ１３または１４が呼出されるように設定しておく。そして、スーパマーケット等で物を購入して支払いをする場合には、そのスーパマーケット等のレジスタ１９から自己の銀行口座の呼出指定を行ない、前記⑤，⑥と同様の方法で自己の銀行口座へのアクセスを行なう。なお、自己の銀行口座呼出指定手段としては、設備利用者所有の装置３３から出力された銀行口座呼出指定信号をレジスタ１９から入力し、銀行へ伝送する方法を用いる。

【００６０】また、自動車等のドアの解錠、エンジンの始動等のアクセスは利用対象設備が移動物であるために、公衆回線等の有線系メディアによるデータ通信は不可能であり、衛星通信等の無線系メディアを用いる。

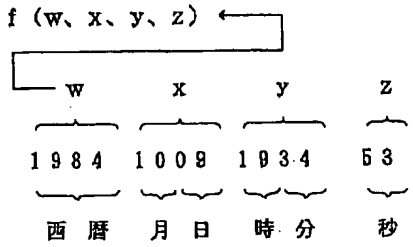
【００６１】次に、前述した個体識別方法を説明する。図５に示すように、ＪＪＹによる時刻標準電波等のコード／データ放送を受信し、その受信信号に基づいて時刻を表示する腕時計により設備利用者所有の装置３３を構成してある。そして、腕時計３３内に記憶されているシークレットルールとしてのシークレット関数（それぞれの腕時計によって相違する）に、その腕時計３３が表示している現在の時刻を入力信号として代入し、答えを算出し、その答えと使用した入力信号のうち秒に相当する部分を識別信号としてアウトプットする。アウトプットの方法は、図６に示すように、まず送信ボタン２１を押

し、腕時計裏面の伝導板からなる信号送出し部２２から手２３にパルス電流として識別信号が一定時間（１０秒間）送り出され、導体である手２３を媒体として、レジスタ１９、コインロッカ１２、自動車２０、キャプテン用端末機１８、電話機、テレテックス用端末機等の識別信号受信部２４へ送信される。送信された識別信号は、個体識別判断を行なう自宅または所定の機関のコンピュータ１３または１４へ送られ、そのコンピュータに予め登録されているシークレットルールとしてのシークレット関数に入力信号を代入して答えを算出し、その答えと識別信号とを比較して正しいか否かを判断し、個体識別を行なう。

【００６２】前記シークレット関数は、三角関数、指数関数等の組合せからなる関数で、４つの変数ｗ、ｘ、ｙ、ｚを有し、以下に示す数１のように、入力信号のそれぞれの部分をｗ、ｘ、ｙ、ｚに代入して答えを算出する。

【００６３】

【数１】



また、外国から我が国へ識別信号を送る場合には、外国の時刻を我が国の時刻に変換した入力信号をシークレット関数に代入する必要がある。

【００６４】図中２５は或る一定の信号を発生する設備利用者所有の指輪型発信機であり、発信機それぞれによって発信信号が相違するもので、前記腕時計３３が、その発信機２５からの所定の信号を受信しているときにのみ識別信号を発信するように構成し、腕時計３３紛失時における他人の悪用を防止する。

【００６５】図中２６は、自己の銀行口座呼出しの際等に使用するキーボードであり、暗証番号をインプットしたり、銀行口座呼出指定信号をアウトプットさせたりするもので、それら信号は、識別信号と同様に信号送出し部２２からアウトプットされる。

【００６６】なお、前記腕時計３３は、コード／データ放送による信号に基づいて逐一表示時刻との誤差が修正されるように構成されているものであり、腕時計３３内に組込まれるプログラムのフローチャートを図７に示す。

【００６７】また、シークレットルールが登録されているコンピュータ１３または１４に組込まれるプログラムのフローチャートを図８に示す。この図８のプログラム中、「許容値Ｋ」は、腕時計３３内で識別信号を算出するために要する時間やシークレットルール登録コンピュータ１３または１４までのデータ通信所有時間等を考慮した遅延時間であり、たとえば３秒等の短い時間である。また、今回の識別信号受信時刻が前回の識別信号受信時刻から前記許容値Ｋ秒以上経過していることをアクセス許容条件に加えている理由は、識別信号ＡとＮＺが送信されたときから前記許容値Ｋ秒以内においてシステム悪用者が前記識別信号をＡとＮＺを記録してシークレットルール登録コンピュータ１３または１４に送信して不当に設備へのアクセスを行なう不都合を防止するためである。

【００６８】次に、この個体識別システムの発明の別実施例を説明する。

（１）　前記シークレット関数への入力信号として、現在の時刻を用いる代わりに、コード／データ放送に基づいて経時的に増加または減少する全国共通または全世界の共通の数字を用いる。その場合に、レジスタ１９、キャプテン用端末機１８等の識別信号入力端末から前記入力信号用数字を発信してもよく、設備利用者所有の装置３３への送信手段は、電波送信またはケーブルの接続のどちらでもよい。

【００６９】さらに、設備利用者所有の装置３３は腕時計に限らず、電子卓上計算機等の個人端末であれば何でもよい。

【００７０】（２）　入力信号として、未だに使用されたことのないものを用いる選択使用手段として、過去に用いられたことのある入力信号を拒絶する機能をシークレットルール登録コンピュータ１３または１４に付加する。この場合のシークレットルール登録コンピュータ１３または１４に組込むプログラム、設備利用者所有の装置３３に組込むプログラムのそれぞれのフローチャートを図９（Ａ）、（Ｂ）に示す。

【００７１】（３）　指名手配者等の捜索対象人間のシークレットルールを登録し、そのシークレットルール登録コンピュータに識別信号が伝送されてきた場合に、その識別信号を入力した端末機に場所通達指令信号を返送し、その端末機から警察のコンピュータ等に端末機設置場所を表示する信号を伝送するように構成する。

【００７２】（４）　前記個体識別のために用いられたシークレットルールを前述のディジタル署名システムの発明に用いた秘密ルールによって肩代わりさせる。つまり、或る人物が所有する秘密ルールを、前記ディジタル署名システムと個体識別システムとに兼用使用する。

【００７３】

【発明の効果】本発明は、署名者が所有するパーソナル端末装置に秘密ルールが記憶されており、署名対象である送信データがそのパーソナル端末装置に入力され、パーソナル端末装置内部において前記秘密ルールに従ったアルゴリズムにより入力データが変換され、その変換データがパーソナル端末装置から出力されてディジタル署

13

名として用いられるために、前記秘密ルールおよびその秘密ルールを用いた送信データの変換がパーソナル端末装置から外部に漏れることが極力防止できる。つまり、パーソナル端末装置に記憶されている前記秘密ルールを外部のコンピュータ等の演算装置に一旦出力し、その演算装置により送信データの変換をする場合には、その演算装置に秘密ルールが記憶されて登録されてしまうおそれがあり、前記秘密ルールが外部に漏れる危険性が大きいが、本発明においては、署名者が所有するパーソナル端末装置に記憶されている前記秘密ルールに従ったアルゴリズムにより、そのパーソナル端末装置内部で送信データの変換が行なわれるために、前記秘密ルールが外部に漏れる危険性を極力防止し得るのである。その結果、ディジタル署名を行なうに際し、署名者が所有する秘密ルールの秘密性を極力守ることができ、その秘密ルールの外部への漏洩を極力防止できるディジタル署名システムを提供し得るに至った。

14

【図面の簡単な説明】

【図１】斜視図である。

【図２】フローチャートである。

【図３】作用説明図である。

【図４】作用説明図である。

【図５】作用説明図である。

【図６】斜視図である。

【図７】フローチャートである。

【図８】フローチャートである。

【図９】（A）（B）はそれぞれフローチャートである。

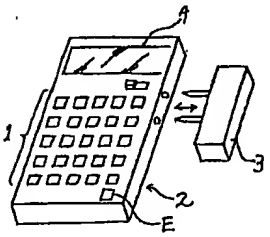
【図１０】パーソナル端末装置の制御回路図である。

【図１１】本発明の背景となるディジタル署名システムの概略を説明する説明図である。

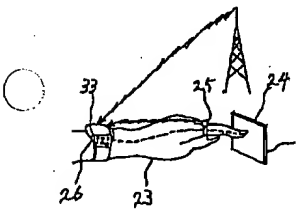
【符号の説明】

３は、パーソナル端末装置、２は入力装置、１はキーボード、２５は発信機である。

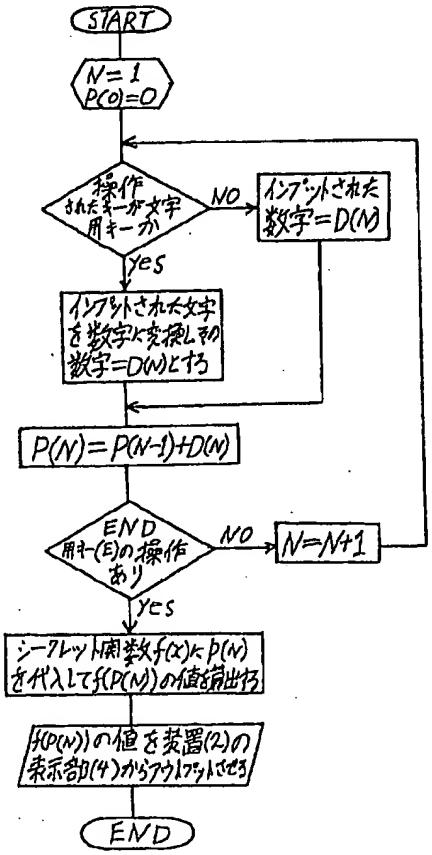
【図１】



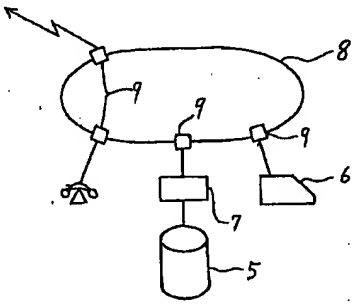
【図５】



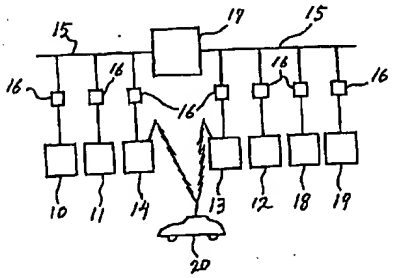
【図２】



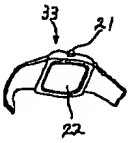
【図３】



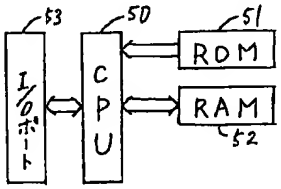
【図４】



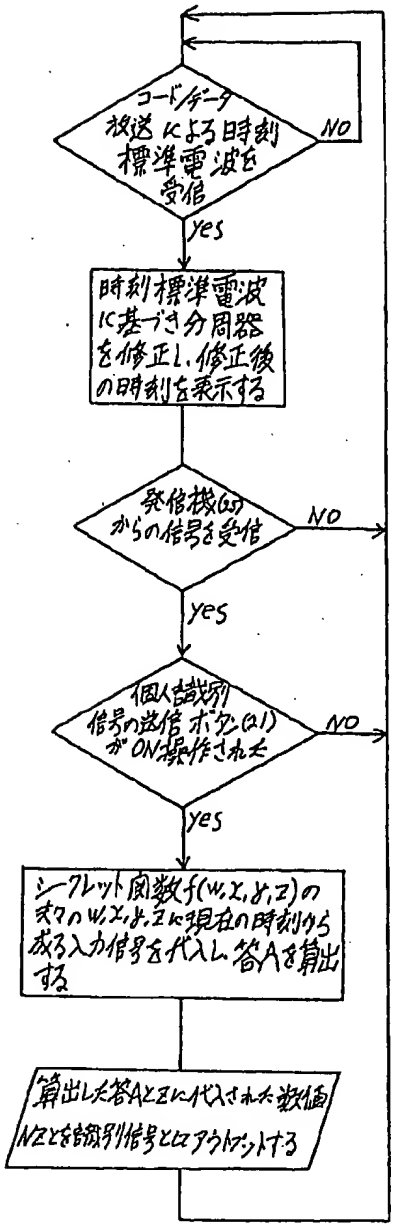
【図６】



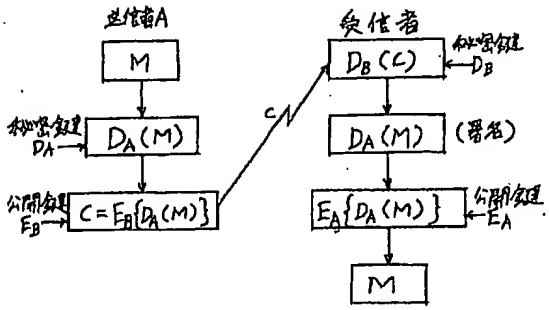
【図１０】



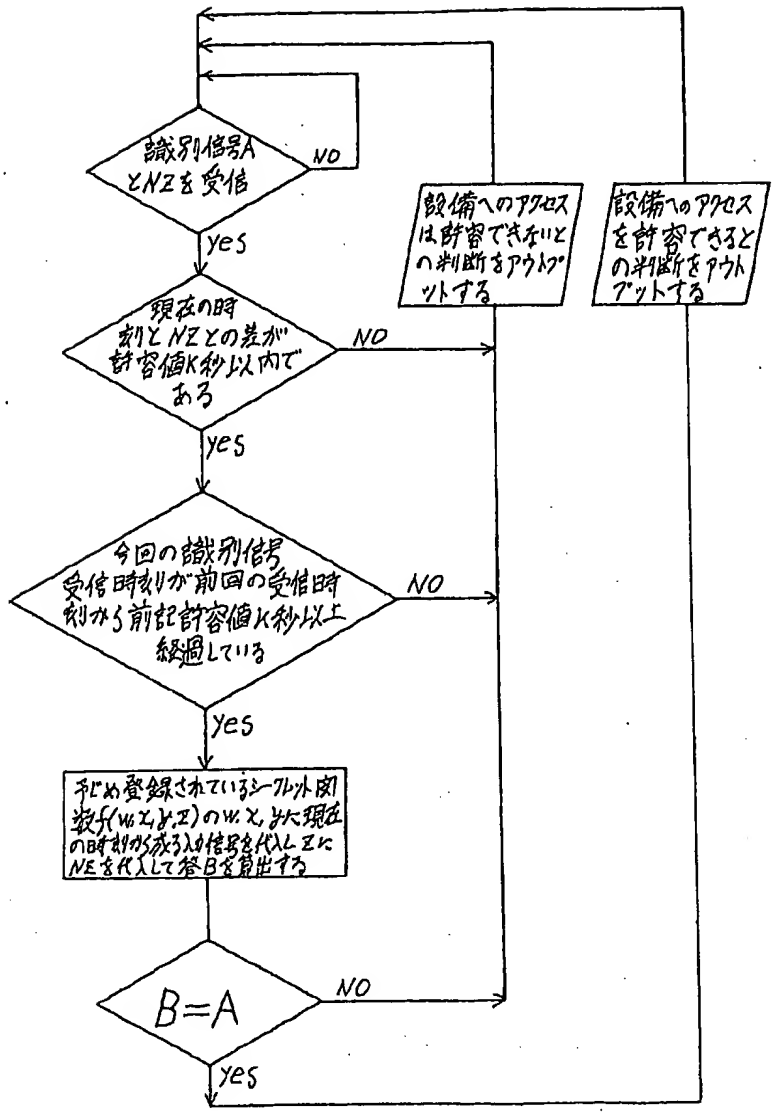
【図7】



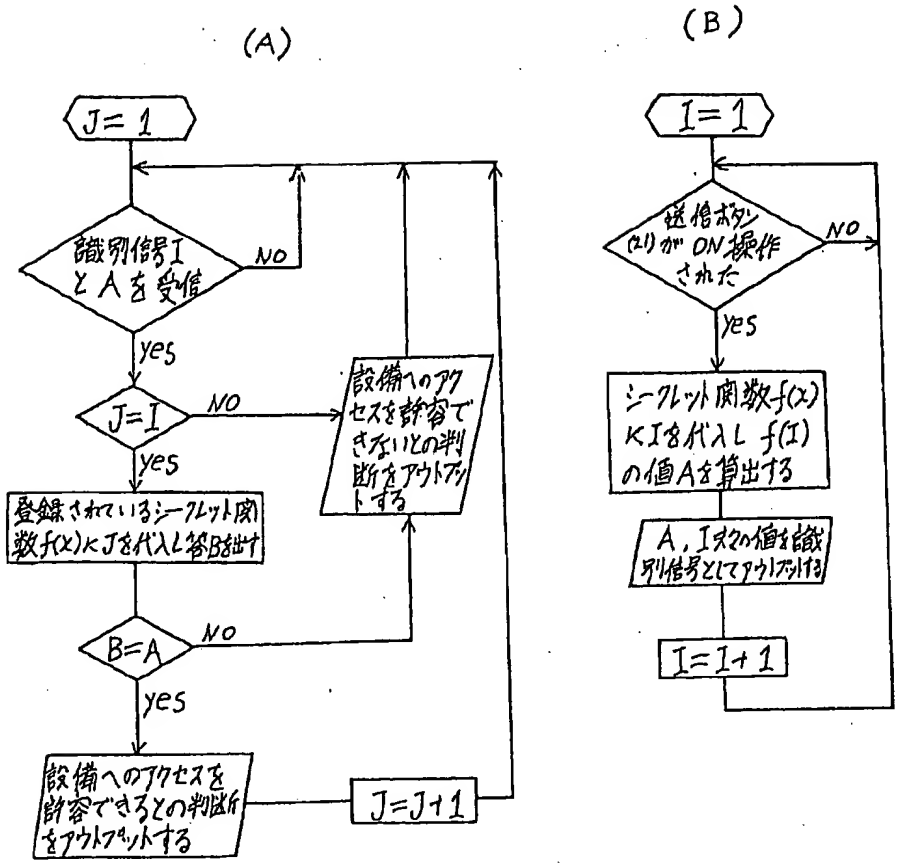
【図11】



【図8】


識別信号A
とNZを受信
NO
yes
現在の時
刻とNZとの差が
許容値K秒以内で
ある
NO
yes
今回の識別信号
受信時刻が前回の受信時
刻から前記許容値K秒以上
経過している
NO
yes
予じめ登録されているシーケント関
数f(W,Z,Y,Z)のW,X,Yに現在
の時刻から成る入力信号を代入しZに
NEを代入して答Bを算出する
B=A
NO
yes
設備へのアクセス
は許容できないと
の判断をアウトプ
ットする
設備へのアクセス
を許容できると
の判断をアウト
プットする

【図9】


(A)
J=1
識別信号I
とAを受信
NO
yes
J=I
NO
設備へのアクセスを許容できないとの判断をアウトプットする
yes
登録されているシークレット関数f(x)にJを代入し答Bを出す
B=A
NO
yes
設備へのアクセスを許容できるとの判断をアウトプットする
J=J+1
(B)
I=1
送信ボタンがON操作された
NO
yes
シークレット関数f(x)にIを代入しf(I)の値Aを算出する
A，Iその値を識別信号としてアウトプットする
I=I+1